Trend 5

From Me to We:

Take the mission further with multiparty systems

FEDERAL TECHNOLOGY VISION 2021

Accenture Federal Services

accenture

Federal agencies have long collaborated with stakeholders and outside partners to achieve specific mission or business outcomes, whether to ensure quality in supply chains, share health records, administer benefits, exchange data, or track funds, just to name a few.

Agencies typically approach these collaborations as the authority, responsible for everything from collecting, managing, and maintaining the necessary data to issuing regulations and policy and enforcing compliance among all stakeholders. Today, however, we are beginning to see this paradigm give way to a new model in which multiparty collaborations achieve their objectives by relying upon an underpinning of mutual trust in shared data and a shared data infrastructure whose immutability and transparency are assured.

The advancing state of blockchain, distributed ledger, distributed database, tokenization, and other similar technologies and capabilities make this pivot possible. But at the core of MPS is the realization that the capabilities of a single agency can only stretch so far—business and mission outcomes that would otherwise be unattainable or attainable only at great expense require the combined capabilities and expertise of multiple organizations working in collaboration on a basis of trust. This trend is occurring in great haste across many commercial sectors, such as banking and finance, supply chain management, healthcare, and real estate, among others. But we also see many federal agencies exploring multiparty system (MPS) approaches and putting them into practice as a way to bring greater efficiency, transparency, accountability, security, interoperability, and confidence to their transactions and processes.

There are countless use cases where federal agencies can employ MPS approaches to deliver significant benefits. But to do so, agency leaders will need to re-examine their traditional practices and approaches.

The power of multiparty systems in an era of epic disruption

At the height of the COVID-19 pandemic, Singapore introduced a blockchain-based medical record system.[1] The "Digital Health Passport" let individuals store medical documents in a secure digital wallet. At a time when monitoring the spread of the virus was crucial, the system allowed the government to easily track the levels of infection and eliminated the need for paper records—all while maintaining individuals' privacy. It also gave people verifiable test results and the hospital discharge papers they needed in order to be cleared for work. In other words, it put a clean and trusted bill of health right at everyone's fingertips—and was used more than 1.5 million times in its first four months alone.

This isn't an isolated story. From contact tracing to frictionless payments, governments and companies around the world have doubled down in exploring and investing in MPS approaches. With the benefit of hindsight, the rapid adoption of multiparty systems isn't all that surprising. COVID-19 made it clear that organizations can't navigate through disruption and uncertainty alone. One of the biggest impacts of the pandemic was how it unveiled global enterprise fragility, leaving companies and government agencies alike cut off from their partners, scrambling for answers, and needing to build new, trustworthy relationships.

75% of federal executives reported their organization faced a moderate to complete supply chain disruption due to COVID-19.

For instance, the pandemic demanded that enterprises develop deeper insight into how people and things were moving, without sacrificing privacy or efficiency—a capability that existing systems were not ready to meet. Across many areas, multiparty systems quickly shifted from ambitious undertakings to desperately needed solutions.

Take, for example, the global airline industry, which has the common goal of resuming airline travel in a safe, controlled, streamlined way as more people get vaccinated against COVID-19. To accomplish this, the International Air Transport Association (IATA), representing almost 300 airlines around the world, launched the IATA Travel Pass, a mobile app that enables travelers to store and manage verified information on their COVID-19 tests and vaccines. Alan Murray Hayden, IATA's head of airport, passenger, and security products, noted that there are two main issues with confirming whether people wanting to fly have been tested or vaccinated: confidence and scalability. "When people do get tested, they turn up with a piece of paper and people don't have confidence in that. And the second point is that agents still need to check these paper documents. And that's what we are really trying to solve with this solution," Hayden said in an interview published in Future Travel Experience.[2]

The IATA Travel Pass, which employs blockchain technology, is a tool for travelers, but—because it relies upon open standards, an important ingredient for MPS interoperability—it also communicates with governments, airlines, test centers, and vaccination providers to get verified information to those who need it in a safe and secure manner. "This is the beauty of the technology we're using; it puts the passenger in complete control of their data. There's no central database and nobody can hack it. The passenger owns their data and they share it with the airline," Hayden said. IATA hopes the new app will help mitigate bottlenecks that may arise once passenger numbers bounce back. "Replacing the paper documents with electronic version[s] and using the verifiable credential will allow airlines to push all of this off airport[s], so passengers arrive completely documented," Hayden added.[3]

> The pandemic demanded that enterprises develop deeper insight into how people and things were moving, without sacrificing privacy or efficiency.

Trials with the IATA Travel Pass demonstrates a key value of multiparty systems, which is that each party to the arrangement is responsible for a function for which it is highly qualified, either because it alone possesses authoritative data critical to the MPS functionality or it has needed domain expertise or both. The result is a capability and value that would be very difficult, if not impossible, for one organization to achieve on its own.

For example, an individual passenger with the Travel Pass app would scan the chip on their passport to retrieve passport information, enter their flight information, and be provided a list of nearby verified lab centers where they can get a COVID test. Those test results are then uploaded to the app by the lab. IATA's Timatic database and rules engine then automatically correlates that information with the COVID travel restrictions in place at the traveler's destination and verifies whether that passenger is authorized to travel. That verification can then be presented to the airline upon arrival at the airport. Each participating party—the passenger, the passport, the lab, IATA, and the airline carrying the passenger—engages in an interoperable, decentralized trust framework that revolves around a secure data foundation.

In the post-COVID era, government and commercial enterprises face an imperative to forge a resilient, adaptable, and trustworthy foundation for their existing and future partnerships. There's opportunity here: Disruption has upended our expectations for ecosystems and ambitious enterprises are creating new standards for industry. Coordinated, strategic ecosystem partnerships will set government agencies and companies up to address today's disruptions and be better prepared to weather new ones, but they'll also enable ways to create new interactions and tackle complex problems.

Multiparty systems: Combining trust and collaboration to reformulate federal operations

It takes a lot of time, energy, and resources to manage something as complex as, say, a supply chain for electronic components for military weapons systems.

It requires dedicated staff, IT resources, and budgets. The data at the center of it must be continuously updated, reconciled, backed up, and verified. Even then, it can be hard to trust the data due to gaps, irregularities, human error, or even outright tampering. Visibility into that data can also be challenging—stakeholders may have to synchronize their data to make sure they are all tracking accurate, up-to-date information.

Multiparty systems offer federal agencies a way to achieve business and mission outcomes that would otherwise be unattainable or attainable only through great expense in staff, budget, and time resources. While the benefits of MPS arrangements can be significant, it's important to understand that they begin with the core understanding that those benefits are attainable only by pooling the resources and contributions of many organizations.

Take, for example, the Defense Logistics Agency, which has a need to counter the threat of counterfeit and nonconforming parts entering the Defense Department's supply chain. For this purpose, DLA created the Counterfeit Detection & Avoidance Program (CDAP), which aims to ensure that critical electronic components are procured from reputable vendors and manufacturers. To do this, the program relies upon a pre-qualification of vendors and a post-award review process to inform decisions about whether components are safe to procure. These processes are highly manual and require a great deal of correspondence with vendors.

In 2019, DLA saw the potential to achieve these same goals using digital processes that would deliver greater automation, efficiency, and anti-fraud protections. But to do this, DLA leaders realized they needed to start by assembling a larger ecosystem of organizations that have a mutual stake in the outcome and obtain their participation. A diverse stakeholder group was formed that included CDAP representatives; DLA's warehousing team in Warren, Ohio; a test laboratory team responsible for inspecting electronic microcircuits received through the CDAP process; original equipment manufacturers (OEMs) and original component manufacturers (OCMs); and distributors and resellers. Together, these organizations formed a Trusted Working Group, which drafted a vision for an improved, more efficient method of collaborating to complete CDAP requirements.[4]

As with the DLA example, any MPS arrangement begins first with a focus on thinking outside of one's organizational boundaries for solutions to thorny, complex challenges. It's about asking, "where do I fit in the ecosystem of my mission outcomes, where do I contribute to other organizations' mission outcomes, and how do I form those partnerships to get needed efficiencies to deliver better value to my constituents?" It is these partnerships and assembled ecosystems that will allow agencies to make challenging business and mission outcomes more easily and quickly attainable with less expense. But there are other key benefits that come from MPS approaches as well:

- They institutionalize trust in their data and processes, presenting all parties involved a single source of truth; and

- They spread the burden of collecting, validating, storing, managing, adjudicating, and maintaining all the data required to manage a complex process.

There are myriad other benefits as well, depending on the use case involved. For supply chain traceability, for example, it dramatically accelerates the time—from several days down to a few seconds—to identify an impacted product, whether tainted lettuce or a recalled drug, and alert downstream partners.[5] For supply chain integrity, it improves safety and security.[6] For grants management, benefits include greater transparency, reduced financial burden, and improved customer experience.[7]

MPSs accomplish all this by enabling federal agencies to shift their approach from *managing the complex process* by themselves to *orchestrating an ecosystem* that manages the process together as a shared, trusted, transparent undertaking. Put simply, MPS helps us trust the data we rely on and trust the transactions we conduct without having to centralize it all into one big system that we manage ourselves.

The appeal is pretty clear: Orchestrating an ecosystem—especially when using automation and artificial intelligence—takes a lot less time, energy, and resources than managing the whole process and all of the underlying systems and data. For example, DLA ultimately designed and implemented a prototype application, called Blockchain Traceability for the Counterfeit Detection and Avoidance, that enabled CDAP and its vendors to collaborate closely on the same platform. The application included several novel features, including: a near real-time credential verification button; immutable records of vendor qualifications and related documentation; and a process for onboarding vendors with a blockchain-based decentralized identifier. These features, along with several other quality of life improvements such as automated email services, field-level validations, and help text provided the CDAP stakeholders with a greatly enhanced digital process compared to the current state.[8]

As with all MPS arrangements, once all of the participating parties contribute their respective domain expertise and data, much of which is done automatically, the MPS uses data analytics to automate the intended outcomes. Those outcomes could include spotting an anomalous component in a supply chain, streamlining an administrative process, or verifying someone's eligibility for benefits. Moreover, the result is more trustworthy, transparent, and accountable than with traditional approaches.

Those features—trust, transparency, accountability—are a byproduct of the technology underlying any MPS. These technologies include distributed databases, distributed ledgers, and digital tokens. Of these, blockchain—a type of distributed ledger technology—is by far the most widely used. While there are many varieties of blockchain, it is, at its core, an immutable and encrypted ledger system that is distributed across a decentralized network of independent computers which can update in near real time. The beauty of a distributed ledger system is that it allows any participating user to prove the record is uncorrupted. Think of it as a strongly encrypted, verified, shared Google Document in which data can be added but never changed and in which each entry depends on a logical relationship to all preceding entries and is agreed upon by everyone who has access to it.

Because it operates as a shared, synchronized and geographically disbursed database with no centralized data storage, the system is designed to remove the "single point of failure" risk present in many other systems. Plus, blockchain is intrinsically a highly secure architecture. Each data entry creates one block within a chain of blocks, and each block is hashed by a set of unique characters derived from information contained inside that block. Every block of data added to the chain has its own unique hash. If any unauthorized changes to the data are made, it becomes immediately apparent to all participating parties.

Many federal experts see tremendous promise in blockchain and other MPS technologies as a tool to advance government business and mission needs. "Data sharing through a blockchain can increase trust in detailed accounts, improve seamless communication, reduce data variation and mitigate friction points when information transfer needs to be timely and actionable," wrote Brig. Gen. Mark Simerly, commander of the Defense Logistics Agency Troop Support in Philadelphia, and Dan Keenaghan, then-process compliance director for audit and process improvement at DLA Troop Support, Philadelphia, in an article about the value of blockchain in military logistics.[9]

In broad terms, MPS arrangements excel at tracking assets, exchanging data, and automating processes. Consequently, we see them in practice most frequently with use cases that involve many federal tasks and functions: accounting, auditing, data provenance, supply chain management, finance, titling, Internet of Things (IoT) management, and digital identity, among others.

18% of federal executives report their organizations are scaling their multiparty systems this year with another 15% beginning to experiment.

Many agencies are already exploring multiparty systems

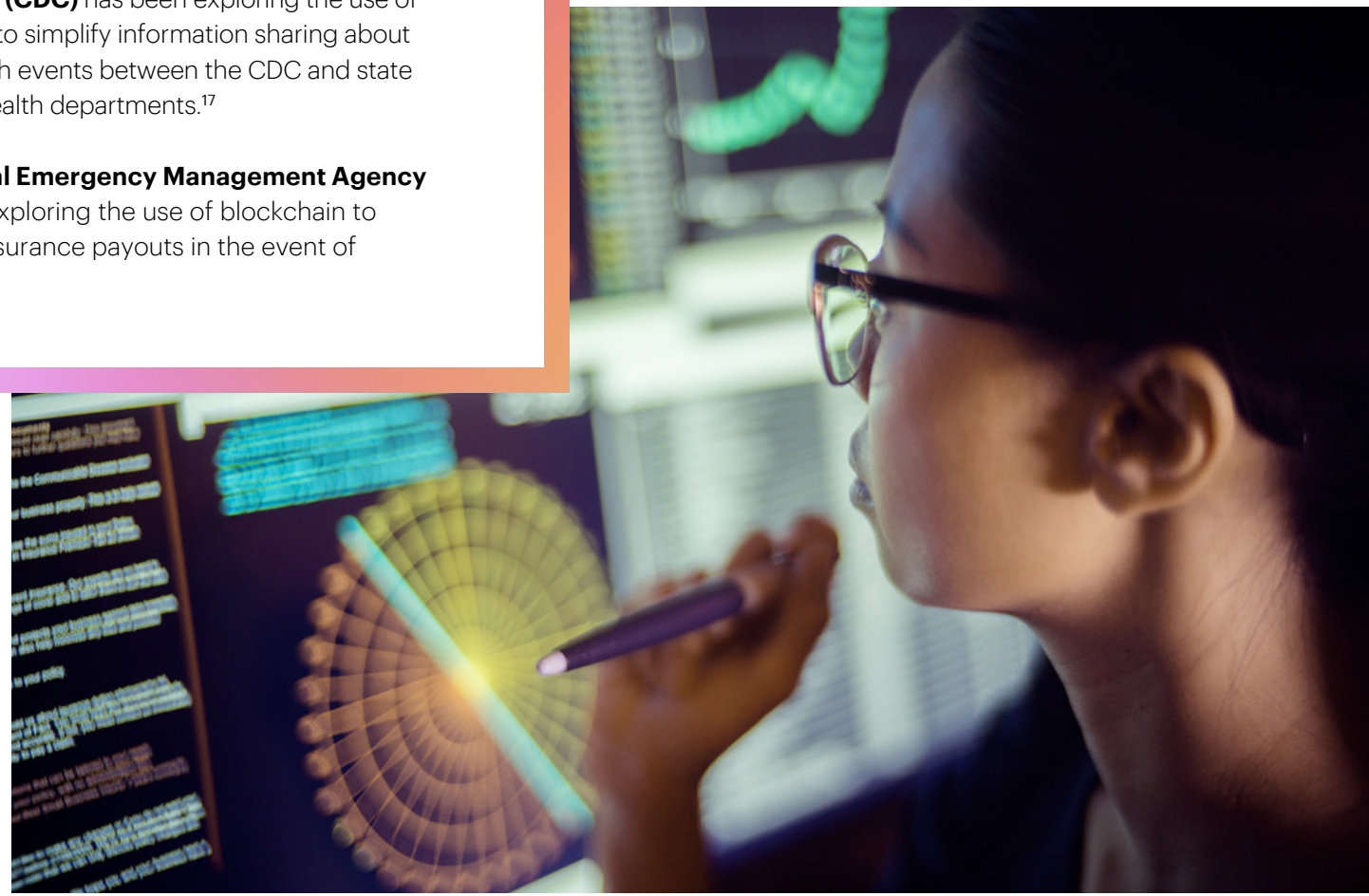
Given the many benefits of MPS approaches, it's easy to see why so many organizations are exploring their use in addressing a wide array of complex challenges. For example, Customs and Border Protection (CBP) conducted a successful proof-of-concept to demonstrate blockchain's ability to help border agents rapidly and cost-effectively determine whether imported products are infringing on the intellectual property rights (IPR) of American companies.[10] The proof-of-concept showed that blockchain connected product data correctly to the product and to the product license, resulting in fewer physical examinations of products being imported, according to CBP. Seven companies participated in the test and were able to communicate with other participants using their unique blockchain, regardless of different software used by each party, due to the program's open global standards and approaches. This demonstration may offer new tools in CBP's fight against imported counterfeit goods.

Similarly, the Treasury Department has been working since 2017 on a project to test how blockchain can improve the grants payment process. Treasury has been working with the National Science Foundation, which has a large research grant portfolio, San Diego State University, and Duke University. In this project, Treasury creates a digital asset (or *token*) that is embedded in a blockchain that contains the details and payments found in letters of credit that are sent to grantees. So rather than having to rely on regular reporting from the prime and sub-grantee recipients, NSF can use the blockchain to track the grant payments and ensure that the terms of the grant are being followed and that the whole transaction is more secure. This frees up grantees of some of their reporting requirements.[11]

The Health and Human Services Department pioneered the federal government's first use of blockchain in 2018 when it received an authority to operate a blockchain- and AI-powered tool called HHS Accelerate. The tool uses blockchain to link together and affirm the integrity of current data from multiple contract-writing systems and about 100,000 contracts that represent nearly $25 billion in annual spend and updates that data every 24 hours. The tool's purpose is to create full visibility into the prices the department pays vendors for products and services so it has greater negotiating power to reduce its procurement spend. Pulling together and analyzing the data needed to negotiate a department-wide strategic sourcing procurement used to take months of work—with Accelerate, it takes seconds.[12] By 2020, the Accelerate tool had saved the department an estimated $30 million over five years with just one large procurement and more savings were anticipated with other large procurement deals in the works.[13]

These are just a few examples. But many other agencies are also incorporating blockchain and other MPS technologies for various use cases. To list a few:

- **The U.S. Air Force** is testing blockchain's ability to secure industrial IoT networks from unauthorized tampering or cyber attacks.[14]
- **CBP** is exploring whether blockchain can ensure that the data coming from cameras and sensors posted along the border has not been spoofed or tampered with in any way.[15]
- **The Naval Air Warfare Center** in San Diego is deploying a blockchain-based messaging and transaction platform that will be used to share technical and provenance information between stakeholders—whether on land, at sea, or air-based—in a trusted and secure environment.[16]
- **The Centers for Disease Control and Prevention (CDC)** has been exploring the use of blockchain to simplify information sharing about public health events between the CDC and state and local health departments.[17]
- **The Federal Emergency Management Agency (FEMA)** is exploring the use of blockchain to expedite insurance payouts in the event of a disaster.[18]



Explore further

Fortify:

When clouds collide

Rapid digitalization during the pandemic has paved the way for enterprises to rethink partnerships. The intrinsic capabilities of the cloud—the scale, the API-enabled connectedness, the advanced cloud-native applications—have long been gateways to deep collaboration, and now that enterprises of all stripes have accelerated their cloud transformations all at once, there is an abundance of potential partners.

Simultaneous and accelerated change is creating a network effect that will lead to new services, business models, and value generation. As organizations interconnect their cloud assets in exciting new ways, new partnerships will be forged and traditional boundaries challenged. The most immediate step federal agencies need to take is to make sure they have the foundation needed to participate in and lead the new digital ecosystems that are already emerging.

A good example of this can be found at the Homeland Security Department. The department's first blockchain proof-of-concept (POC) was conducted in 2018 by CBP, which tested whether the technology could assist border agents as they process imported goods subject to the North American Free Trade Agreement (NAFTA) and Central America Free Trade Agreement (CAFTA). The POC was a joint effort that also had significant participation from importers, CBP auditors, import and entry specialists, CBP legal and policy personnel, technology companies, and suppliers. The POC proved 100 percent successful, demonstrating that blockchain technology can be implemented in a U.S. customs environment, improve the processing and tracking of trade documents, facilitate interaction with multiple entities, enable better auditability, reduce paperwork, and expedite processing.[19]

But that success—and the success of numerous other MPS proof of concepts to follow—owes itself to DHS laying the needed groundwork with a capable, flexible cloud foundation; open, pre-defined standards for easier integration; and needed in-house and contracted technical expertise. "Historically, when new technologies or solutions are incorporated into legacy systems, there are obstacles that create slowdowns as workarounds are developed so that the systems mesh properly," said Anil John, technical director at DHS' Silicon Valley Innovation Program, which is part of the department's Science and Technology Directorate (S&T). "However, through the use of globally acceptable and implemented specifications and standards, we are addressing and removing those interoperability hurdles before deployment. That way our industry partners and government components can hit the ground running."[20]

That spadework was critical because the integration challenge to make the POC possible was considerable: The resulting blockchain integrated with 10 different systems and three different types of blockchain software. In addition, trading partners participating in the POC relied upon different operational environments—some ran their systems on Amazon Web Services, others in the IBM Cloud, others in custom Docker environments, and still others in Open Stack environments. Engineers with DHS' Digital Bazaar worked through these challenges and achieved interoperability using HTTP API connections.[21]

After CBP's successful demonstration, S&T helped the U.S. Citizenship and Immigration Services test blockchain's ability to improve the way it issues citizenship, immigration, and employment work-status authorization documents to be faster, more accurate, and more secure. It also helped the Transportation Security Administration explore whether blockchain could help secure, automate, and speed up the credential validation process at checkpoints.[22]

In general, commercial sectors are outpacing federal adoption of MPS technologies such as blockchain—but not in every case. CBP noted in its after-action report following the POC that many trading companies had not yet adopted blockchain, which "may prevent rapid adoption of this technology."[23] But this relative immaturity of the marketplace presents federal agencies with a golden opportunity. "If government entities join the blockchain revolution early on, they have an opportunity to drive the change, rather than to react and adapt to systems established by others," wrote Svetlana Angert in her 2019 thesis examining the lessons learned of the CBP proof of concept while at the Naval Postgraduate School in Monterey, Calif. She noted that DHS' early effort to set the interoperability specifications and standards for blockchain was critical to success, and she urged other agencies to take the initiative in doing this as well. "CBP can facilitate future coordination, implementation, and creation of global blockchain standards necessary in international trade," she wrote.[24]

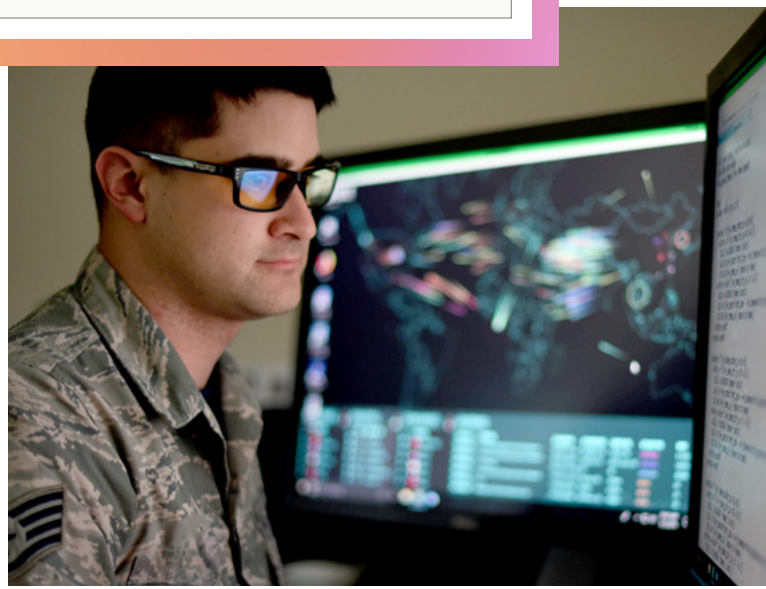
As the DHS example demonstrates, the cloud is fundamental to unlocking the power of MPS.

In addition to the growing number of blockchain platforms emerging in the marketplace, many of the larger federal cloud services, including AWS, Microsoft, and Google, offer blockchain services. Also, many of the major enterprise resource planning (ERP) vendors have begun adding blockchain capabilities to their offerings.

The Defense Department's Defense Information Systems Agency (DISA) is going even further by creating a Blockchain-as-a-Service (BlaaS) offering that can be used by DoD support agencies and military services to streamline the path to production for blockchain systems in the future.[25]

As partners combine their digital efforts, the resulting ecosystems are generating novel solutions, just as we saw with CBP's free trade agreement blockchain demonstration. Successful leaders are adopting an ecosystem mindset that feeds through business and technology strategy, eschewing the traditional organizational boundaries of the past. MPS makes clear that technology-based ecosystems are the foundation for future growth and leadership, and agencies will need to invest in the needed platforms to set those ecosystems motion.

91% of federal executives agree that to be agile and resilient, their organizations need to fast forward their digital transformation with cloud at its core.

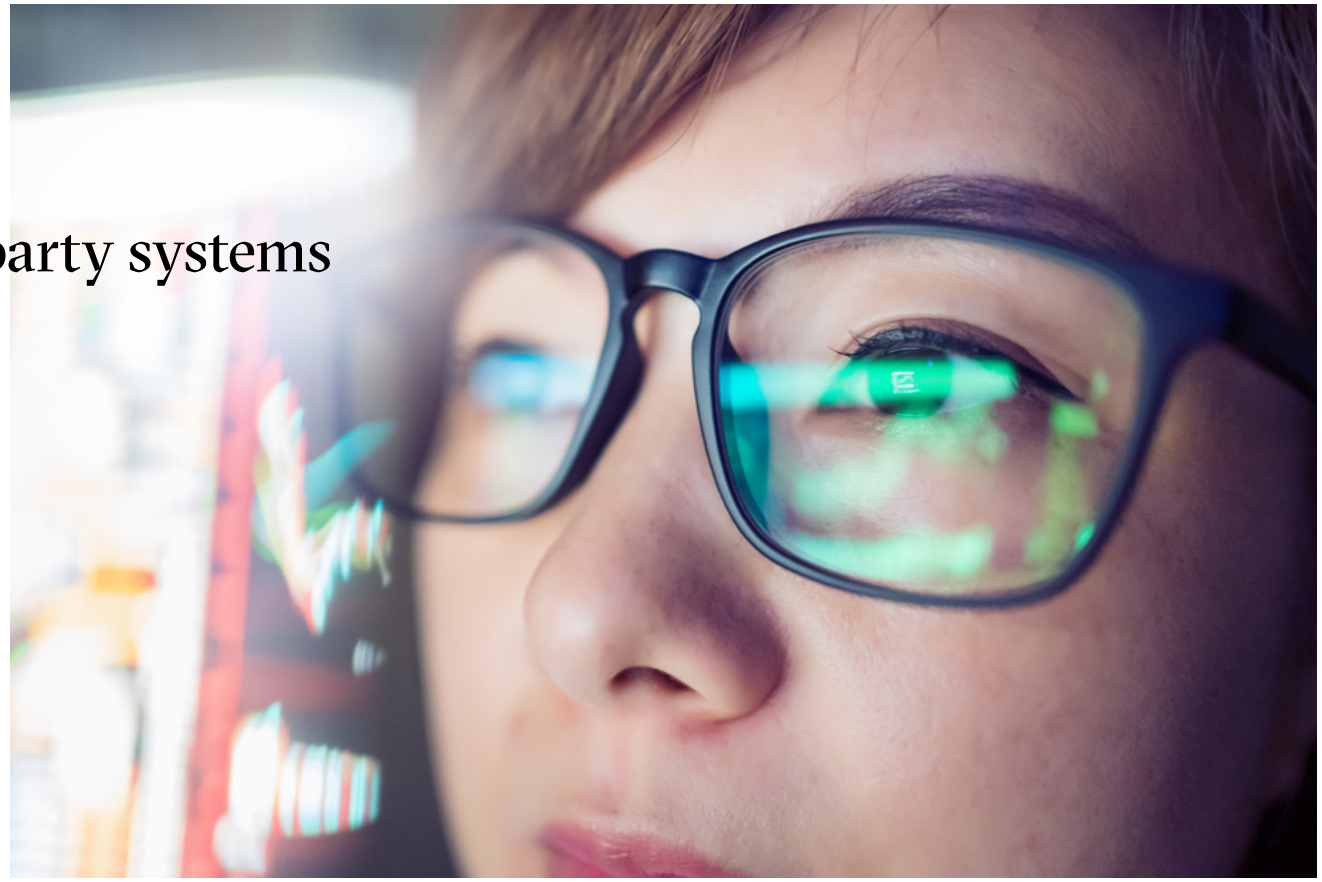


The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

Extend:

Natural federal use cases for multiparty systems

Having a cloud foundation is key to benefiting from the value of MPS approaches, but so is the need to shift one's thinking to better envision the vast possibilities MPS can bring to federal mission and business operations.



Again, DHS offers a good example here. Technologists there had been tracking the progress of distributed ledger technology for years and saw significant promise in its applications for many DHS business and mission operations. "Throughout the HSE [Homeland Security Enterprise], agencies issue entitlements, attestations and certifications," said a July 2019 press release issued by the department's Science and Technology Directorate. "The holders of those credentials might be an individual, organization or product, but from the HSE perspective, they all have at least one thing in common—the documentation must be quickly verified, extremely robust and resistant to tampering. Paper-based, manual verification solutions are slow, non-centralized and pose [a] greater risk of forgery and counterfeiting. Blockchain is tailor-made to address and mitigate these security and speed issues."[26] It was this insight that drove the department to launch a string of proof of concepts with blockchain.

Perhaps the broadest category of MPS use cases can be found where federal agencies are already engaged in collaborations, networks, and consortiums, either with external organizations or other agencies or both. These can include ecosystems that revolve around supply chains and logistics, financial services, disaster response and assistance, industry regulation and inspection, transportation, research and development, and more. Numerous agencies are already exploring whether MPS arrangements can help them prevent counterfeit components in supply chains, secure military communications, accelerate recalls of tainted food and pharmaceuticals, and dispense disaster assistance more rapidly.[27]

"More than 62 million power grid items were provided to Puerto Rico in the wake of the Category 5 Hurricane Maria," said DLA's Simerly and Keenaghan of DLA Troop Support in Philadelphia in their October–December 2019 issue of *Army Sustainment*. DLA supports FEMA and the U.S. Army Corps of Engineers by leveraging hundreds of contracts to mobilize millions of equipment pieces that support humanitarian assistance and disaster relief efforts. "Although the mission was a success, an assessment of the end-to-end processes uncovered multiple delays, miscommunications, excessive travel costs, a lack of comprehensive end-to-end visibility, and many wasted hours for manual corrections. Research suggested the possibilities for adaptation and innovation through blockchain could increase effective communication of requirements, planning movement and flexibility, monitoring third party delivery and in-transit visibility timelines, compliance with regulatory demands, and transparency for audit. Cost reductions are anticipated in regards [to] information lags, duplication, personnel, movement times, storage, and inventory losses. These efficiencies enabled through blockchain technology would provide real, measurable savings and increase the efficacy of life-saving and recovery efforts."[28]

Another example of how MPS approaches fit naturally into many existing ecosystems can be found in the world of unmanned aerial systems, or UASs. The commercialization of UASes is exploding—there are already nearly four times as many UAS as registered manned aircraft. And many federal agencies, along with the fast-growing UAS industry, are aggressively exploring how blockchain and other MPS technologies can address the many challenges being anticipated with the rapid growth in commercial UAS operations.

According to a 2020 Department of Transportation report, companies and federal agencies are considering embedding blockchain and other distributed ledger technologies into a wide assortment of UAS functions and activities to make them secure, transparent, trackable, authenticated, and trusted. These include identity management, traffic management, conflict management, flight authorization, flight data recorders, insurance, regulation compliance, fleet security, and cybersecurity.[29] "Blockchain is poised to transform the way we think about and analyze safety data," said Regina Houston, Chief of the Aviation Safety Management Systems Division, U.S. DOT Volpe National Transportation Systems Center. "This is particularly exciting for unmanned aerial vehicles. Blockchain can be part of the solution to collecting and sharing reliable data about drones. When you combine machine learning with the data blockchain can provide on UAS registration, accountability, and tracking, an entire world becomes available for drone safety analysis, decision making, and even regulation."[30]

In short, areas where policy, regulatory, and governance frameworks cross over federal organizations and commercial industries are prime venues for MPS applications. A big part of getting MPS off the ground is having disparate organizations agree upon a governance framework on how things will operate; but, in many cases, those already exist in many federal environments, which gives federal agencies a distinct advantage in getting started, finding common ground, and bringing those ecosystems together.

91% of federal executives say multiparty systems will enable their ecosystems to forge a more resilient and adaptable foundation to create new value with their organization's partners.

Reinvent:

A new perspective on value

It helps when enterprises embarking on MPS undertakings have a fuller sense of the value that partnership can bring. Consider an area where MPS is having extraordinary impact: money.

The first large-scale popular implementation of an MPS technology was Bitcoin in 2009. A decentralized digital currency that is not controlled by a central bank, Bitcoin can be exchanged from one user to another through a peer-to-peer network without the need for intermediaries. Bitcoin transactions are verified by network nodes through cryptography and recorded in a blockchain. Its success has touched off a wave of similar cryptocurrencies, all built on decentralized peer-to-peer networks—today, there are more than 4,000 cryptocurrencies in existence, including Ethereum, Litecoin, Cardano, Polkadot, Bitcoin Cash, and Stellar, to name a few.[31] While many of them have little to no following or trading volume, some are immensely popular among dedicated user communities and investors.

This brave new world of cryptocurrencies is prompting many federal agencies to study the potential ramifications they may have on their missions and business operations. For example, numerous federal investigative organizations—including the Treasury Department's Office of Global Targeting, the IRS Criminal Investigation (IRS-CI), the Postal Inspection Service, and the Army Criminal Investigation Command—are reviewing their procedures and exploring solutions that can help them track digital currency transactions that involve individuals, entities, and organizations that are blocked from conducting business with Americans or that are potentially criminal in nature.[32]

In addition, the Energy Department is looking for ways to detect hidden malware that enlists infected computers to mine for digital currencies. Bitcoin mining is the process by which new bitcoins are entered into circulation, and it requires very sophisticated computers that can solve highly complex math problems. If successful, mining can reap cryptocurrency tokens without having to pay for them. Cryptocurrency mining malware is a growing problem for the department's National Labs, which use High-Performance Computing (HPC) applications to conduct complex research.[33]

But the flood of new cryptocurrencies has also catalyzed many governments and central banks around the world to think anew about the need to update their government-backed currencies for the digital age. As of January 2021, 86 percent of the world's central banks were considering issuing "Central Bank Digital Currencies" (CBDCs), according to a report by the Bank of International Settlements (BIS).[34] A CBDC is a digital form of a country's fiat currency; instead of printing money, the central bank issues electronic coins or accounts backed by the full faith and credit of the government. Because CBDCs are the liability of the central bank, the government must maintain reserves and deposits to back it up.

CBDCs are attractive to central banks for many reasons. First, being digital, the maintenance and handling expenses of CBDCs—printing, managing, and transferring, for example—are far less than for hard currencies. Also, people can have access to money on their smart phones, making it more accessible and safer. And because there is a digital track record for every unit of currency, there is greater transparency and more checks on illicit activity.[35] But there are risks as well: our regulatory processes, financial transaction systems, and payment systems are not updated to deal with these new forms of money. Also, the proliferation of digital currencies could hamper the ability of policymakers to track cross-border monetary flows, presenting challenges concerning the use of sanctions and economic policy tools.

In October 2020, the International Monetary Fund (IMF) began working with the Group of 20 to establish a set of standards for CBDCs.[36] Accenture has been working with central banks across the globe as they explore their digital programs and it is likely we will see the first CBDCs come to fruition in the next 12 to 24 months.[37] For instance, The Digital Dollar Project—a non-profit partnership between Accenture and the Digital Dollar Foundation—is advancing a collaborative framework for developing a CBDC in the United States, and the central bank in Sweden, the Riksbank, is piloting the e-krona to test its viability.[38] The project will launch at least five pilot programs over the next 12 months with interested stakeholders and DDP participants to measure the value of and inform the future design of a U.S. CBDC, or "digital dollar."

CBDC efforts worldwide demonstrate why businesses need to have multiparty systems at the forefront of their innovation agenda—and also why leaders need to take a considered approach with their efforts. People are at the center of these ecosystems, and the technology needs to support their ambitions—not overshadow them. Recognizing this, the World Economic Forum, along with Accenture, established a set of guidelines called the Presidio Principles to help guide experimentation with multiparty systems.[39] The guidelines span four categories and include the principles that every participant should have rights to information about the system; that individuals should be able to own and manage their data, and have their data protected in accordance with recognized technical security standards; and that participants should have the information they need in order to pursue effective recourse. The goal of these principles is to ensure that multiparty systems are providing for a more equitable and inclusive future.

At their zenith, MPSs will transform the world. If you've hesitated to explore a full ecosystem approach, now is the time to recognize the opportunity; if you've already been exploring, it's time to move beyond small-scale implementation and become a leading partner in shaping tomorrow's government operations.

Decision points

Fortify: How are digitally led partnerships driving value for your enterprise?

- 2020 saw a surge of federal agencies expanding their embrace of digital platforms to accelerate business and mission operations. Review what platforms your agency—and its stakeholders—leaned on most in the last year.
- Take advantage of cloud solutions and have a strategy for using these solutions to enhance ecosystem collaboration. Find other agency, industry, commercial, and academic partners that have shared interests that overlap with your mission or business and explore collaborating to bring greater value and security to your operations.

Extend: Is your agency ready to participate in multiparty systems?

- Multiparty systems are steadily growing in adoption. Designate a team to scan prominent MPSs emerging in your mission or business area, assess their current and long-term impacts, and gauge your enterprise's relative preparedness to engage them. Make understanding the technology, identifying technical partners and providers, and addressing skills gaps a priority.
- MPS is more than technology—it reshapes business practices and models. Determine if MPS is the right solution by evaluating the business case that will drive your participation. This could include areas where transactional data has yet to be digitized or complex networks that would benefit from a common and trusted platform.

Reinvent: Which business relationships will be transformed by the growth of multiparty systems?

- Think beyond the walls of the enterprise. Interview strategic partners to understand their exposure to multiparty systems. Consider running strategic foresight exercises with these partners to evaluate the need and impact of a multiparty system.
- Consider joining industry consortiums or establishing a working group of inter-enterprise partners. Create the process for assessing the value of any MPS strategy against the benefit to all participants, not just the enterprise in isolation.

Author

Marty Hebeler
Managing Director
Armed Forces Technology Lead
Accenture Federal Services

Exploring Tech Vision

For over twenty years, the Accenture Technology Vision has identified the most important emerging technology trends impacting businesses, governments, and society over the next three years. What sets it apart is its focus on the underlying forces behind each trend as well as the frank advice it offers on how enterprises should respond. The Accenture Technology Vision is produced by Accenture Labs and Accenture Research with input from over one hundred Accenture leaders and more than two dozen external experts. It also incorporates the findings of a global survey of over 6,000 enterprise leaders.

This year's global report, Leaders Wanted, examines how the world responded to the unprecedented stresses and challenges created by the COVID-19 pandemic. What we learned is that many enterprises are far more agile than they thought. Their challenge going forward is accelerating their digital transformation to meet the new expectations left in the pandemic's wake.

The Accenture Federal Technology Vision 2021 applies these trends to the unique demands and challenges facing the U.S. federal government. It builds upon insight from more than 50 Accenture Federal Services experts as well as survey data from two hundred federal program, business and IT leaders.

Readers can assess the accuracy and relevancy of our predictions for the federal government by reviewing last year's report. Key trends in the Accenture Federal Technology Vision 2020 included the I in Experience, AI and Me, the Dilemma of Smart Things, Robots in the Wild, and Innovation DNA.

References

1 https://www.zdnet.com/article/singapore-touts-blockchain-use-in-covid-19-data-management/

2 https://www.futuretravelexperience.com/2021/01/how-iata-travel-pass-is-using-blockchain-technology-to-keep-passengers-in-control-of-their-data/

3 https://www.futuretravelexperience.com/2021/01/how-iata-travel-pass-is-using-blockchain-technology-to-keep-passengers-in-control-of-their-data/

4 https://apps.dtic.mil/sti/pdfs/AD1108292.pdf

5 https://www.ibm.com/blogs/blockchain/2020/05/how-the-fda-is-piloting-blockchain-for-the-pharmaceutical-supply-chain/

https://www.ibm.com/downloads/cas/9V2LRYG5?utm_medium=OSocial&utm_source=Blog&utm_content=000020YK&utm_term=10005803&utm_id=How-the-FDA-is-piloting-blockchain-for-the-pharmaceutical-supply-chain-In-Text&cm_mmc=OSocial_Blog-_-Blockchain+and+Strategic+Alliances_Blockchain-_-WW_WW-_-How-the-FDA-is-piloting-blockchain-for-the-pharmaceutical-supply-chain-In-Text&cm_mmca1=000020YK&cm_mmca2=10005803

6 https://www.afcea.org/content/navy-raises-anchor-blockchain

https://atloa.org/er-combating-counterfeit-parts-in-the-dod-supply-chain/

7 https://c16fcadc-43cf-4d42-9af1-75c9979362e2.filesusr.com/ugd/418ed8_55d10914398b49efb13cb4d890409597.pdf

8 https://apps.dtic.mil/sti/pdfs/AD1108292.pdf

9 https://www.army.mil/article/227943/blockchain_for_military_logistics

10 https://www.cbp.gov/sites/default/files/assets/documents/2020-Mar/IPR%20POC%20Report%20-%20Final%20V2.pdf

https://www.cbp.gov/newsroom/national-media-release/cbp-leverages-blockchain-innovation-protect-american-business

11 https://gcn.com/articles/2020/01/13/treasury-nsf-blockchain-grants-tracking.aspx

https://gcn.com/articles/2019/12/06/blockchain-nsf-grant-payments.aspx

https://gcn.com/Articles/2018/02/22/FIT-blockchain-RPA.aspx

https://www.fiscal.treasury.gov/fit/updates/deee-blockchain-fit-update.html

12 https://federalnewsnetwork.com/technology-main/2018/12/hhs-blockchain-ai-project-gets-go-ahead-to-use-live-agency-acquisition-data/

https://fedtechmagazine.com/article/2020/02/qa-hhs-cio-brings-procurement-expertise-it-table

13 https://www.meritalk.com/articles/blockchain-saving-hhs-30m-on-first-accelerate-contract/

14 https://www.iottechtrends.com/how-zero-trust-blockchain-tech-secure-air-force/

15 https://gcn.com/articles/2018/07/02/cbp-blockchain-sensor-data.aspx?m=1

16 https://blog.simbachain.com/blog/simba-chain-awarded-contract-from-us-navy-to-deploy-secure-messaging-solutions

17 https://www.fiercehealthcare.com/mobile/cdc-blockchain-public-health-surveillance-data-sharing

https://www.technologyreview.com/2017/10/02/148864/why-the-cdc-wants-in-on-blockchain/

18 https://www.ledgerinsights.com/fema-blockchain-disaster-insurance-parametric/

https://cointelegraph.com/news/fema-suggests-blockchain-based-registry-to-improve-disaster-insurance-payouts

19 https://www.cbp.gov/sites/default/files/assets/documents/2019-Oct/Final-NAFTA-CAFTA-Report.pdf

20 https://www.dhs.gov/science-and-technology/news/2019/07/09/snapshot-blockchain-and-dhs

21 https://www.cbp.gov/sites/default/files/assets/documents/2019-Oct/Final-NAFTA-CAFTA-Report.pdf

22 https://www.dhs.gov/science-and-technology/news/2019/07/09/snapshot-blockchain-and-dhs

23 https://www.cbp.gov/sites/default/files/assets/documents/2019-Oct/Final-NAFTA-CAFTA-Report.pdf

24 Angert, S. (2019). Blockchain Technology Implementation in the U.S. Customs Environment [Master's thesis, Naval Postgraduate School]. Homeland Security Digital Library.

25 https://disa.mil/-/media/Files/DISA/Fact-Sheets/Summer-Look-Book-June2020.ashx

26 https://www.dhs.gov/science-and-technology/news/2019/07/09/snapshot-blockchain-and-dhs

27 https://atloa.org/er-combating-counterfeit-parts-in-the-dod-supply-chain/

https://apps.dtic.mil/sti/pdfs/AD1108292.pdf

https://gcn.com/articles/2020/03/13/blockchain-ip-military-logistics-coronavirus.aspx

https://federalnewsnetwork.com/technology-main/2019/06/for-hhs-blockchain-means-faster-id-management-and-safer-mangoes/

https://www.ibm.com/blogs/blockchain/2020/05/how-the-fda-is-piloting-blockchain-for-the-pharmaceutical-supply-chain/

28 https://www.army.mil/article/227943/blockchain_for_military_logistics

29 https://rosap.ntl.bts.gov/view/dot/48789

30 https://rosap.ntl.bts.gov/view/dot/48789

31 https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/

32 https://www.nextgov.com/emerging-tech/2021/05/treasury-office-seeks-tools-trace-cryptocurrency-linked-sanctions-list/173894/

https://www.nextgov.com/emerging-tech/2021/03/watchdog-review-how-postal-inspectors-handle-cryptocurrency/172983/

https://www.nextgov.com/emerging-tech/2020/07/army-investigative-unit-looks-detect-and-trace-cryptocurrency-transactions/166844/

https://www.nextgov.com/emerging-tech/2020/09/irs-wants-be-able-trace-untraceable-digital-currencies/168305/

33 https://www.nextgov.com/emerging-tech/2021/02/national-lab-creates-technology-detect-cryptocurrency-mining-malware/172304/

34 https://www.bis.org/publ/bppdf/bispap114.pdf

35 https://www.atlanticcouncil.org/blogs/econographics/the-rise-of-central-bank-digital-currencies/

36 https://www.fsb.org/2020/10/regulation-supervision-and-oversightof-global-stablecoin-arrangements/

37 https://www.bis.org/publ/othp33.pdf

38 https://www.digitaldollarproject.org/

https://www.technologyreview.com/2020/02/20/906146/sweden-riksbank-ekrona-blockchain/

39 https://www.weforum.org/communities/presidio-principles

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 569,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at **www.accenture.com**

About Accenture Federal Services

Accenture Federal Services, a wholly owned subsidiary of Accenture, brings together mission expertise with proven innovation and leading practices to help the federal government do the extraordinary things it takes to create a better future for all of us. We are passionate about partnering with clients, going beyond the bold future we collectively imagine, to create real and enduring change for our country and our communities. We deliver new value and advantage that lasts, drawing on the full power of our partners and Accenture. Learn more at **www.accenture.com**

Contributors

John Conley
Steve Watkins
Riley Panko

About Accenture Labs

Accenture Labs incubates and prototypes new concepts through applied R&D projects that are expected to have a significant impact on business and society. Our dedicated team of technologists and researchers work with leaders across the company and external partners to imagine and invent the future. Accenture Labs is located in seven key research hubs around the world: San Francisco, CA; Washington, D.C.; Dublin, Ireland; Sophia Antipolis, France; Herzliya, Israel; Bangalore, India; Shenzhen, China and Nano Labs across the globe. The Labs collaborates extensively with Accenture's network of nearly 400 innovation centers, studios and centers of excellence to deliver cutting-edge research, insights, and solutions to clients where they operate and live. For more information, please visit **www.accenture.com/labs**

About Accenture Research

Accenture Research shapes trends and creates data-driven insights about the most pressing issues global organizations face. Combining the power of innovative research techniques with a deep understanding of our clients' industries, our team of 300 researchers and analysts spans 20 countries and publishes hundreds of reports, articles and points of view every year. Our thought-provoking research—supported by proprietary data and partnerships with leading organizations, such as MIT and Harvard—guides our innovations and allows us to transform theories and fresh ideas into real-world solutions for our clients. For more information, visit **www.accenture.com/research**